Software Requirements Specification

(SRS)

for the ECPN CSCI

Version 1.0.6

10/10/96

Contract No. F19628-93-D-0019
CDRL Sequence No. B003

Prepared for:

Defense Information Systems Agency (DISA)
45335 Vintage Park Plaza
Sterling, VA 20166-6701

Prepared by:

Inter-National Research Institute, Inc.
12350 Jefferson Avenue, Suite 380
Newport News, Virginia 23602

Document Control No. ECPN SRS.2 10/10/96

Software Requirements Specification

(SRS)

for the ECPN CSCI

Version 1.0.6

10/10/96

Prepared for:

Defense Information Systems Agency (DISA)
45335 Vintage Park Plaza
Sterling, VA 20166-6701

Prepared by:

Inter-National Research Institute, Inc.
12350 Jefferson Avenue, Suite 380
Newport News, Virginia 23602

Authenticated by _____   Approved by _____
        (Contracting Agency)   (Contractor)

Date _____   Date_____

The following trademarks and registered trademarks are mentioned in this document. Within the text of this document, the appropriate symbol for a trademark (™) or a registered trademark (®) appears after the first occurrence of each item.

AT&T is a registered trademark of AT&T Information Systems, Incorporated.

Cleo is a registered trademark of Interface Systems, Incorporated.

HP is a trademark of Hewlett-Packard Company.

IBM is a registered trademark of International Business Machines, Corporation.

Kermit is a registered trademark of Henson and Associates, Inc.

Sun is a trademark of Sun MicroSystems, Inc.

UNIX is a registered trademark in the Uninted States and other countries, licensed exclusively through X/Open Company Limited.

VAX is a registered trademark of Digital Equipment Corporation.

Table of Contents

Section 1
SCOPE

This Software Requirements Specification (SRS) applies to Electronic Commerce Processing Node (ECPN), which is a Computer Software Configuration Item (CSCI) of the system identified as Electronic Commerce/Electronic Data Interchange (EC/EDI). The purpose of this SRS is to specify the requirements for ECPN and the methods to be used to ensure that each requirement has been met.

ECPN will be developed in phases using a spiral method for rapid evolutionary development. Accordingly, the initial ECPN requirements will be refined during the course of its development and any additional requirements will be identified with each succeeding phase of the system. New and revised requirements and their source(s) will be added to this SRS as they become known.

1.1 Identification

The system identifier for ECPN has not yet been assigned. The purpose of ECPN is to provide NEP/Gateway enhancement to a platform environment that has more capability and functionality. The enhancement must ensure interoperability, economies of scale, and compliance to standards by the Department of Defense (DoD) and Federal Program Management Office (PMO). The current NEP and Gateway architecture and functionality are to be merged and redesignated as an ECPN.

1.2 System Overview

The EC/EDI system receives, processes, stores, and routes computer-to-computer messages for business transactions. Additionally, it monitors networks and alerts users of problem messages or communications trouble while providing an audit trail of system operations.

ECPN is being developed by Inter-National Research Institute (INRI) specifically for the EC/EDI system. The role of ECPN is to enhance the current EC/EDI Network Entry Point (NEP)/Gateway system. The fundamental objectives of this effort are to:

◆ Maintain rigorous accountability end-to-end within the NEP/Gateway processing, with no single point of failure that could cause loss or non-delivery of data.

◆ Automation of the processes required to place DISA EC/EDI into a high volume production environment; should include periodic automated reconciliation mechanisms to ensure that no deliveries are missed.

◆ Eliminate the UNIX® scripts and provide enhanced functionality in executable code.

◆ Enhance NEP/Gateway functionality by providing a transition from batch store/forward capability to single transaction mode.

◆ Implement basic Oracle RDBMS archival capability.

◆ Provide for backup archival, information retrieval, usage reporting and audit trails.

◆ Provide basic retransmission and recovery as well as status monitoring.

◆ Provide for automated notification of communication failure and restore and provide status monitoring.

1.3   Document Overview

This document follows the standards set forth in *Military Standard Software Development and Documentation* (MIL-STD-498) and in the Data Item Description (DID) for an SRS (DI-IPSC-81433), as tailored by INRI.

The following is an overview of each section of this SRS:

Section 1	Scope	States the purpose of the EC/EDI system ; describes the role of ECPN within EC/EDI; and states the purpose of this SRS.
Section 2	Referenced Documents	Lists the documents applicable to this SRS.
Section 3	Requirements	Specifies the requirements for ECPN. These requirements constitute the characteristics of ECPN that are the conditions for its acceptance.
Section 4	Qualification Provisions	Specifies the methods for qualifying that ECPN meets each of the requirements described in Section 3.0.
Section 5	Requirements Traceability	Describes the traceability between and among ECPN requirements in this SRS and the EC/EDI system requirements.
Section 6	Notes	Defines the acronyms and abbreviations used in this SRS.

This page has been intentionally left blank.

Section 2
REFERENCED DOCUMENTS

The following subsections describe the documentation applicable to this SRS. In the event of a later version of a referenced document being issued, the later version shall supersede the referenced version.

◆ *Data Item Description (DID) for an SRS* (DI-IPSC-81433).

◆ *Military Standard Software Development and Documentation* (MIL-STD-498), Department of Defense, 5 December 1994.

This page has been intentionally left blank.

Section 3
REQUIREMENTS

The following subsections specify the requirements for ECPN. These requirements constitute the characteristics of ECPN that are the conditions for its acceptance.

3.1 Required States and Modes

Text forthcoming.

3.10 Computer Resource Requirements

The following subsections specify the computer resource requirements of ECPN.

3.10.1 Computer Hardware Requirements

Text forthcoming, as applicable.

3.10.2 Computer Hardware Resource Utilization Requirements

Text forthcoming, as applicable.

3.10.3 Computer Software Requirements

Text forthcoming, as applicable.

3.10.4 Computer Communications Requirements

Text forthcoming, as applicable.

3.11 Software Quality Factors

This section specifies ECPN requirements concerned with software quality factors identified in the contract or derived from a higher-level specification.

Text forthcoming, as applicable.

3.12 Design and Implementation Constraints

This section specifies the requirements that constrain the design and implementation of ECPN.

Text forthcoming, as applicable.

3.13 Personnel-Related Requirements

This section specifies ECPN requirements included to accommodate the number, skill levels, duty cycles, training needs, or other information about the personnel who will use or support ECPN.

Text forthcoming, as applicable.

3.14 Training-Related Requirements

This section specifies ECPN requirements pertaining to training.

Text forthcoming, as applicable.

3.15 Logistics-Related Requirements

This section specifies ECPN requirements concerned with logistics considerations.

Text forthcoming, as applicable.

3.16 Other Requirements

This section specifies any additional ECPN requirements not specified in the previous sections.

Text forthcoming, as applicable.

3.17 Packing Requirements

This section specifies the requirements for packing, labeling, and handling ECPN for delivery.

Text forthcoming, as applicable.

3.18 Precedence and Critically of Requirements

This section specifies the order of precedence, critically, or assigned weight indicating the relative importance of the requirements in this SRS.

Text forthcoming, as applicable.

This page has been intentionally left blank.

3.2 CSCI Capability Requirements

The following subsections itemize the requirements associated with each capability of ECPN.

3.2.1 Capability Requirement - 001

ECPN shall provide a communications interface capable of using Kermit® /ZMODEM protocol for dial-up type connections.

A user interface shall allow configuration of the following communications parameters:

- ◆ transmit cycle rate
- ◆ destination node type (VAN, Gateway, or NEP)
- ◆ transmit batched/non-batched messages
- ◆ phone number
- ◆ login name/password
- ◆ dial time-out
- ◆ transmit packet size
- ◆ receive packet size
- ◆ baud rate
- ◆ parity
- ◆ remote in directory
- ◆ remote out directory
- ◆ tty device
- ◆ byte size
- ◆ receive end-of-packet character
- ◆ escape character
- ◆ window size
- ◆ block check

The user interface shall also allow multiple channels to be configured and shall allow easy activation/deactivation of the interface when necessary.

3.2.2 Capability Requirement - 002

ECPN shall provide a communications interface capable of using FTP protocol for network type connections.

A user interface shall allow configuration of the following communications parameters:

- ◆ transmit cycle rate
- ◆ destination node type (VAN, Gateway, or NEP)
- ◆ transmit batched/non-batched messages
- ◆ remote IP address
- ◆ login name/password
- ◆ remote in directory
- ◆ remote out directory
- ◆ push/push-pull

The user interface shall also allow multiple channels to be configured and shall allow easy activation/deactivation of the interface when necessary.

3.2.3 Capability Requirement - 003

ECPN shall provide a communications interface capable of using Cleo® protocol for dial-up mainframe connections.

Background: Currently, several sites depend on the Cleo software package to allow the NEP to interface with IBM® mainframes using synchronous modems. The only hardware platform currently at the NEP that supports this package is an AT&T® 3B2, which creates a severe performance bottleneck to NEP operations.

A user interface shall allow configuration of the following communications parameters:

- transmit cycle rate
- destination node type (VAN, Gateway, or NEP)
- transmit batched/non-batched messages
- phone number
- tty device
- PBX access code
- time delay
- new line suppression
- terminal type
- redial attempts
- transmit record size
- repeat limit
- re-transmit limit
- wait limit
- modem type
- delay limit
- bid limit
- receive limit
- blocking factor
- compression
- protocol

The user interface shall also allow multiple channels to be configured and shall allow easy activation/deactivation of the interface when necessary.

3.2.4 Capability Requirement - 004

ECPN shall provide a communications interface capable of using standard SMTP email protocol for network connections.

A user interface shall allow configuration of the following communications parameters:

◆   transmit cycle rate
◆   destination node type (VAN, Gateway, or NEP)
◆   transmit batched/non-batched messages
◆   user name
◆   destination hostname

The user interface shall also allow multiple channels to be configured (via a configurable database of email addresses) and shall allow easy activation/deactivation of the interface when necessary.

3.2.5 Capability Requirement - 005

ECPN shall provide a communications interface capable of using direct TCP/IP protocol for NEP-to-NEP network type connections.

A user interface shall allow configuration of the following communications parameters:

◆   transmit cycle rate
◆   destination node type (VAN, Gateway, or NEP)
◆   transmit batched/non-batched messages
◆   destination IP address

The user interface shall also allow multiple channels to be configured and shall allow easy activation/deactivation of the interface when necessary.

3.2.6 Capability Requirement - 006

ECPN shall provide a mechanism for defining the site identifier for the local NEP/Gateway.

The NEP/Gateway site identifier shall be used for determination of ISA message routing. Only those ISA messages whose destination address matches the NEP/Gateway site identifier will be routed.

The NEP/Gateway site identifier shall also be used to determine configuration/execution status of the various communications interfaces. An interface will be allowed to run only if it is configured for the local NEP/Gateway identifier.

The system may be allowed to configure multiple NEP/Gateway identifiers when it is necessary to take over the duties of another NEP/Gateway.

3.2.7 Capability Requirement - 007

ECPN shall provide the capability to define characteristics for passively monitored incoming communications sources.

A user interface shall be provided to define those sources of data which are not actively pulled, but instead deposit their data onto the local NEP/Gateway by use of FTP or email. This user interface will update a database of "remote users", which will be checked when polling the directories containing incoming data from the "passive" sources. If the system detects a transfer in progress from one of these sources, it will wait five minutes until checking the directory for that source.

3.2.8 Capability Requirement - 008

ECPN shall provide a means of replicating the active database of transactions between the NEP/Gateway sites.

Initially, this replication may be achieved by use of the autoforwarding table, which will route incoming raw data to the other NEPs/Gateways.

3.2.9 Capability Requirement - 009

ECPN shall provide a means of auditing the flow of a transaction from arrival at the NEP/Gateway to its subsequent routing out of the NEP/Gateway.

This system-level auditing shall be achieved by providing the following features:

◆ a copy of each complete incoming file in the incoming log with time of receipt, customer name, and other header information
◆ a timestamped system alert for message processing failures
◆ a timestamp of message transmission
◆ the ability to view raw received data from message logs
◆ the ability to view raw transmitted data from message logs
◆ the ability to search/sort message logs by critical fields to assist in tracking of messages
◆ a log of all system alerts, with details concerning method of alert, transaction, source, time, etc.

3.2.10 Capability Requirement - 010

ECPN shall provide measures against unauthorized access to the NEP/Gateway functionality and data.

The following measures shall be taken to safeguard the NEP/Gateway:

◆ standard UNIX user/password login protections
◆ TCP wrapper protection to allow only trusted hosts to connect to specific system services
◆ file permissions set to prevent remote users from viewing unauthorized files/directories
◆ all Kermit, Cleo, and ZMODEM communications to be dial-out only
◆ /etc/hosts file to contain the minimum set of host addresses necessary for UNIX system operation
◆ transactions only accepted from AISs/VANs with an explicitly configured communications channel
◆ system-level auditing to preserve the integrity of transactions throughout processing and storage
◆ transmission integrity between ECPN within the ability of selected communications protocol

3.2.11 Capability Requirement - 011

ECPN shall provide a means to enable compression of data for various communications channels. Initially, this functionality will only support the standard UNIX compress.

3.2.12 Capability Requirement - 012

ECPN shall provide email notification of failed transactions.

A transaction may be classified as "failed" for one of the following reasons:

◆ The incoming transaction was interrupted/garbled.
◆ The control numbers are mismatched for corresponding ISA/IEA, GS/GE, or ST/SE line pairs.
◆ The destination from the ISA or GS lines (DODAAC) is unspecified, invalid, or unknown.

The following actions shall occur via email:

◆ An email message stating the type, reason, and point of failure shall be sent to each interested party.
◆ (Optional) The email shall include one or more of the following: ISA/GS/ST control numbers, ISA DTG, group control number, originator, destination DODAAC, and a portion or all of the failed transaction message (i.e., enough information to uniquely identify the transaction and specify the reason for failure).

Ultimately, email notification will be supplemented/replaced by standard X12 997 negative/positive acknowledgments of transactions.

3.2.13 Capability Requirement - 013

ECPN shall perform byte-count validation on incoming/outgoing transactions.

◆ This requirement is only currently applicable for file-level transfers. To implement this means of verification within a data stream would require embedding the byte count within the message, which is not currently supported.
◆ This requirement can only be implemented for interfaces in which we do a "pull" of the file. There is currently no means by which we can assess the original size in bytes of a file that has been "pushed" to us (see above).
◆ When "pulling" a file (via FTP, Kermit, etc.) the file size in bytes on the remote system shall be noted, and then compared to the file size in bytes on the local system after the transfer is complete. Any mismatch shall generate notification of failure (after retrying - see below).
◆ When "pushing" a file to a remote system, the file size locally shall be noted, and then compared to the file size on the remote system after the transfer is complete. Any mismatch shall generate notification of failure (after retrying - see below).
◆ An additional alert shall be added to support notification of a byte count mismatch.
◆ A configurable "retry" feature shall be implemented to allow a certain number of attempts to request transmission of the file before failure is indicated.

3.2.14 Capability Requirement - 014

ECPN shall provide a comprehensive and configurable alerting mechanism to alert the NEP/Gateway administrator of system status and problems in the following general areas:

◆ communications problems (e.g., specific interface problems, WAN problems)
◆ localized system problems (e.g., CPU usage, hardware failure)
◆ invalid/corrupt data (e.g., garbled data, incomplete reception/transmission, invalid formatting of data)

Alert notifications shall be provided by one or more of the following methods:

◆ pop-up windows
◆ email
◆ beeper

Additionally, a centralized log of all alerts generated should be maintained by the ECPN software, with an interface that allows the NEP/Gateway administrator to dismiss those alerts that have been resolved.

3.2.15 Capability Requirement - 015

ECPN shall support configuration of the following alert types:

◆ Cleo communications time-out
◆ FTP communications time-out
◆ Kermit/ZMODEM communications time-out

The system administrator shall be provided with a mechanism to generate alerts based on configurable time-out values for various types of NEP/Gateway processes. The mechanism shall include the capability to set time threshold values for periods of inactivity during the following activities:

◆ Cleo-type dial-up connections
◆ FTP sessions
◆ Kermit/ZMODEM sessions

When these threshold values are reached, an alert shall be generated indicating which system function has exceeded its threshold limit. The alert notification will be handled via the standard configurable means of pop-up window, email or beeper notification.

3.2.16 Capability Requirement - 016

ECPN shall provide beeper notification to the administrator for various alerts.

The system shall be configured to add the capability to provide beeper notification of various alerts in addition to the other methods of alert notification.

A user interface shall be provided to allow the NEP/Gateway administrator to select beeper numbers to be dialed upon receipt of a specified alert. A means of remotely disabling beeper notification shall also be provided.

3.2.17 Capability Requirement - 017

ECPN shall provide an ACK/NAK indicating the success or failure of transaction messages.

In addition to providing X12 997 capability, a low level indication of the successful processing of each incoming and outgoing message shall be present in the message logs.

On the incoming side, the logs shall indicate the following conditions:

◆ message successfully received
◆   message envelope validation failed
◆   message decoded/processed

On the outgoing side, the logs shall indicate the following conditions:

◆ message successfully transmitted
◆   message failed transmission
◆   message pending transmission

This functionality will remain useful in system troubleshooting even after explicit support for 997 messages is implemented.

3.2.18 Capability Requirement - 018

ECPN shall provide the operator with the capability to selectively configure the Incoming/Outgoing Communications Logs.

A user interface shall be provided allowing the creation of new message logs, based on message type. All incoming messages of a specified type shall be allowed to map into the newly created log instead of appearing in the default incoming/outgoing message log. The user shall be able to define a maximum number of messages (up to 50,000) for the log at the time of creation.

The message logs shall be organized to display the following information at a glance for all incoming/outgoing messages:

◆ Transmission Site Name/ID Code
◆ Receiving Site Name/ID Code
◆ ISA Control Number
◆ Solicitation Control Number
◆ ISA Creation Date/Time
◆ Receipt Date/Time
◆ Transmission Date/Time
◆ Transaction Type (e.g., 840, 843, 997, 850, 855, 860, 865, 838, 824, 836, 864, 832, 869, 870, 810, 820)
◆ ISA To/From
◆ GS To/From
◆ PO (Purchase Order) Number
◆ Transaction Control Number
◆ ISA to IEA in/out byte counts
◆ Closing date from BRQ line (for applicable transactions - i.e., 840s)

The message logs shall provide the capability to change the default column headings of the logs to any subset of the aforementioned fields.

The message logs shall provide the capability to sort all messages in ascending/descending order on any field. A future requirement would be to add the capability to do "waterfall sorting", which would allow the user to sort on a number of different fields in succession - the current log sorting removes all memory of a previous sort each time a new column is selected for sorting.

The message logs shall also allow the user to select an entry in the log and view the raw data associated with that entry, for both incoming and outgoing data.

The message logs shall be able to display the log entries of the last 50000 messages received/transmitted. For future use, this capability will need to increase dramatically.

3.2.19 Capability Requirement - 019

ECPN shall implement an Oracle RDBMS as the archive repository.

The initial function of the Oracle RDBMS will be to provide a long-term repository of the incoming and outgoing transactions. The "live" data will be maintained in an organized file structure, with automatic archival to the Oracle RDBMS occurring as a background task so as not to impede real-time communications. The system will provide this archive using on-line rapidly accessible storage.

3.2.20 Capability Requirement - 020

ECPN shall provide the ability to transition outgoing data flow from batch processing to single (event-by-event) transaction mode. The system shall provide the ability to accept incoming data in either batch mode or transaction mode.

Currently, all data flowing in and out of the NEP consists of X12 messages batched into files. The software shall be capable of resegmenting these batch files back into individual X12 messages for display in the message logs. The biggest advantage that this scheme will provide is the ability to segregate a single bad message from a larger batch and still allow processing of the remaining messages.

The software shall be configurable to allow outgoing messages to be sent either individually or in batches, on a channel-by-channel basis. Each channel interface window shall have a toggle that allows the user to select either batch or transaction mode for all outgoing messages. When batch mode is selected, all individual messages will then be batched into a single file/data stream for transmission.

3.2.21 Capability Requirement - 021

ECPN shall implement detailed NEP usage reports.

Currently, statistic reports from the NEP summarize daily transactions by VAN/Gateway/AIS, transaction type, etc. The software shall provide a variety of statistics based upon VAN/Gateway transactions (e.g., number of transactions received via a specific comms channel).

3.2.22 Capability Requirement - 022

ECPN shall provide an automatic status monitor of NEP/Gateway functions.

The software shall provide a mechanism to inform the NEP/Gateway administrator of the operational status of the NEP/Gateway through use of alerts, throughput statistics, and the operational statuses of all communications interfaces.

The system shall use a configurable system of alerts to inform the NEP/Gateway administrator of any critical problems that occur in NEP/Gateway processing (bad data, comms failures, etc.). A user interface shall be provided that allows the NEP/Gateway administrator to configure what alerts are of interest, and what alerting action will be taken.

A window shall indicate the status of all critical NEP/Gateway processes, with a stoplight display indicating if the processes are running, not running, or in an error state.

The incoming/outgoing message logs shall reflect the processing status of a message, indicating success or failure in both reception and transmission.

A window containing a list of all communications interfaces shall be available, with indicators for active status. There shall also be a window that indicates the number of messages sent and received for each interface.

Because the wide-area network will be the primary communications interface, there shall be an expanded set of status information devoted solely to monitoring its performance.   Tools shall be provided to determine the UP/DOWN status of selected sites on the network, using SNMP to provide information about speed of throughput and information about all intermediary points.

3.2.23 Capability Requirement - 023

ECPN shall route transactions according to different address schemes.

The replacement NEP/Gateway software shall provide user configurable routing capabilities, based on a variety of criteria. A user interface shall be provided that will allow creation of routing tables that specify one-to-one routing, one-to-many routing, and many-to-one routing.

The tables shall support routing based on the following criteria:

◆ ISA destination field
◆ GS destination (DODAAC)
◆ incoming comms channel
◆ ISA originator field

To satisfy one-to-one and one-to many routing, the NEP/Gateway administrator will be able to select one or more channels as a destination for messages that meet the specified criteria. Many-to-one routing will be achieved by making multiple entries to the routing table that all have the same output channel selected.

The user interface shall also provide a means to easily activate/deactivate a routing entry.

3.2.24 Capability Requirement - 024

ECPN shall provide ANSI X12 translation services for the SAACONS equivalent UDFs for 840, 843, 997, 850, 855, 860, 865, 838, 824, 836, 864, 832, 869, 870, 810, and 820.

The ECPN software shall be able to receive a message in user-defined format (UDF), corresponding to one of the above message types, and convert it to the proper ANSI X12 format before forwarding the message to its final destination.

Likewise, the software shall be able to receive ANSI X12 for the above message types, and convert them into the proper UDF format (where necessary) before forwarding them to their final destination.

This requirement must be met before the ECPN software will be suitable for operation at Gateway sites. It is not a necessary requirement for NEP operation.

3.2.25 Capability Requirement - 025

ECPN shall provide an extensive archive capability for all incoming and outgoing transactions and other system databases for administrative use.

The system shall provide up to 45 days of archives using on-line rapidly accessible storage, and an indefinite archive using off-line storage. While the goal is 45 days, the actual duration of the available on-line archive depends upon the hardware disk space provided.

For the on-line archives, a mechanism shall be implemented in the standard message logs to allow rapid retrieval of specific subsets of data from the on-line archives.

A user interface shall be provided to allow selection of databases to be archived. A list of available archive devices/media shall be provided, to include: hard disk files, 1/4" cartridge tapes, 4 mm DAT tapes, Exabyte tapes, 3 1/2" floppy diskettes, and 5 1/4" floppy diskettes (where applicable).

A user interface shall be provided to allow retrieval of selected archives from off-line storage media. Archives retrieved from off-line storage shall then be accessible from the standard system location for that database.

The type of off-line media for long-term storage is as yet unspecified, but it must be high-volume, compact, and reasonably rapid-access. Recordable CD jukebox technology may provide a suitable means of archiving.

3.2.26 Capability Requirement - 026

ECPN shall implement a rudimentary retrospective search function for the archives stored in the Oracle RDBMS.

A user interface will be provided in the message logs to enable the operator to specify data values that will direct retrospective searches on the archive database. The operator will be able to conduct searches based on some subset of the following database fields:

◆ Message Type
◆ Group Control Number
◆ Status
◆ Byte Count
◆ ISA Creation Date/Time
◆ Receipt Date/Time
◆ Processing Date/Time
◆ Transmission Date/Time
◆ ISA To/From
◆ ISA Control Number
◆ Transaction Control Number
◆ Solicitation Control Number
◆ Purchase Order Number
◆ Input Channel (Transmission Site Name/ID Code)
◆ Output Channel (Receiving Site Name/ID Code)
◆ GS To/From
◆ Closing Date from BRQ line

3.2.27 Capability Requirement - 027

ECPN shall validate the format of all incoming X12 messages, for applicable segments and fields.

Upon detection of an incorrectly formatted X12 message, the logs shall be updated to indicate that an error was detected during processing. A system alert shall also be generated so that appropriate action may be taken.

The following parameters shall be checked during X12 message validation:

◆ proper ordering/formatting of ISA/IEA envelope
◆ proper ordering/formatting of GS/GE envelope
◆ proper ordering/formatting of ST/SE envelop
◆ valid segment terminators being used
◆ valid destination in ISA line
◆ valid destination in GS line

3.2.28 Capability Requirement - 028

ECPN shall ensure that public messages are forwarded to all applicable parties and shall provide a summary of the VANs/Gateways/AISs that have acknowledged Public messages.

The ECPN software shall provide the capability to properly route messages addressed to PUBLIC via the one-to-many routing scheme to be supported in its X12 routing tables.

3.2.29 Capability Requirement - 029

Because of the current VAN Licensing Agreements, the NEP is responsible for supporting a number of non-standard conventions for handling message traffic from VANs. ECPN shall handle these same contingencies until the licensing agreements can be changed to achieve standardization.

Among the areas to be addressed:

(1) Segment Termination

Currently, the ANSI X12 message specification does not define what character shall be used to separate message segments. It simply says that the same character must be used throughout the message. Consequently, VANs use different segment terminators for their messages.

To compensate, ECPN shall provide the following items:

◆ a user interface to build a table that matches the comms channel for the VAN with the segment terminator it uses
◆ a table to display available segment terminators and their ASCII and octal values
◆ a mapping for the segment terminator on incoming messages to be translated to a common character for all messages internally
◆ automatic segment terminator translation for incoming/outgoing comms as necessary

Ultimately, a single segment terminator should be selected, and all VANs should be standardized.

(2)   Time Zones

ECPN shall provide a table that explains the proper conversion from one time zone (e.g., EST, MST, ZULU, GMT, etc.) to another.

3.3 CSCI External Interface Requirements

The following subsections specify the requirements of ECPN for external interfaces.

3.3.1 Interface Identification and Diagrams

Text forthcoming, as applicable.

3.3.2 (Project-Unique Identifier of Interface)

Text forthcoming, as applicable.

3.4 CSCI Internal Interface Requirements

This section specifies the requirements imposed on interfaces internal to ECPN.

Text forthcoming, as applicable.

3.5 CSCI Internal Data Requirements

The following subsections specify the requirements imposed on data internal to ECPN.

Text forthcoming, as applicable.

3.6 Adaptation Requirements

This section specifies the requirements concerning installation-dependent data to be provided by ECPN, and operational parameters that ECPN is required to use that may vary according to operational needs.

Text forthcoming, as applicable.

3.7 Safety Requirements

This section specifies ECPN requirements concerning preventing or minimizing unintended hazards to personnel, property, and the physical environment.

Text forthcoming, as applicable.

3.8   Security and Privacy Requirements

This section specifies ECPN requirements concerned with maintaining security and privacy.

Text forthcoming, as applicable.

3.9 CSCI Environment Requirements

This section specifies the requirements regarding the environment in which ECPN must operate.
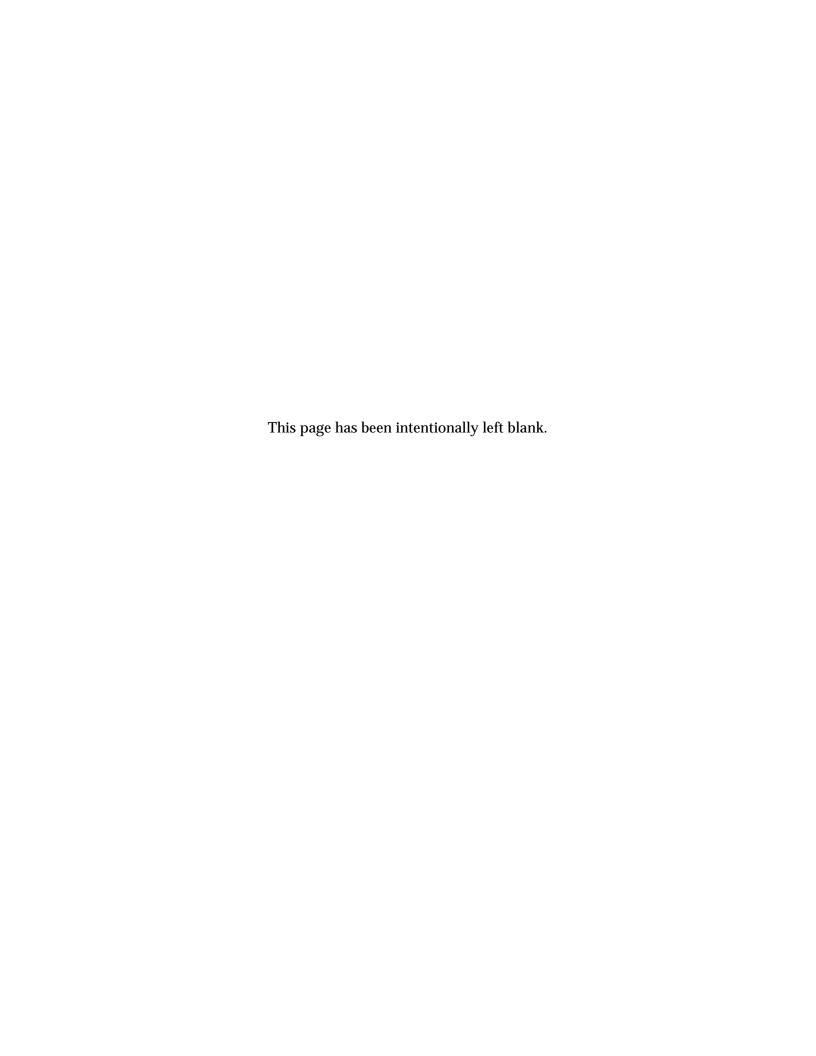
Text forthcoming, as applicable.

Section 4
Qualification Provisions

This section specifies the methods for qualifying that ECPN meets each of the requirements described in Section 3.0.

Text forthcoming, as applicable.

Section 5
Requirements Traceability

This section describes the traceability between and among ECPN requirements in this SRS and the EC/EDI system requirements.

Note that a System/Subsystem Specification (SSS), which normally specifies the system-wide requirements for a system or subsystem, does not exist for the ECPN system. Thus, in accordance with MIL-STD-498, ECPN requirements will be traced to a general "system implementation" requirement for EC/EDI.

Text forthcoming, as applicable.

This page has been intentionally left blank.

Section 6
Notes

The following acronyms and abbreviations appear in this document:

ACK   Acknowledgment
AIS   Automated Information System
ANSI   American National Standards Institute
CD   Compact Disk
CPU   Central Processing Unit
CRC   Cyclical Redundancy Check
CSCI   Computer Software Configuration Item
CTP   Commercial Trading Partner
DID   Data Item Description
DISA   Defense Information Systems Agency
DOD   Department of Defense
DOS   Disk Operating System
DODAAC   DOD Activity Address Code
DTG   Date-Time Group
EC/EDI   Electronic Commerce/Electronic Data Interchange
ECPN   Electronic Commerce Processing Node
FTP   File Transfer Protocol
GE   Functional Group Trailer
GS   Functional Group Header
IBM   International Business Machines
IEA   Interchange Control Trailer
INRI   Inter-National Research Institute
IP   Internet Protocol
ISA   Interchange Control Header
NAK   Negative Acknowledgment
NEP   Network Entry Point
PMO   Program Management Office
PO   Purchase Order
RDBMS   Relational Database Management System
SE   Transaction Set Trailer
SMC   System Monitoring Center
SMTP   Single Mail Transfer Protocol
SNMP   Simple Network Management Protocol
SRS   Software Requirements Specification
SSS   System/Subsystem Specification
ST   Transaction Set Header
UDF   User-Defined Format
VAN   Value Added Network
WAN   Wide Area Network

This page has been intentionally left blank.

This page has been intentionally left blank.